Public Comment Summary Report

Name Collision IPv6 Research Study

Open for Submissions Date:
Monday, 20 October 2025

Closed for Submissions Date:
Monday, 22 December 2025

Summary Report Due Date:
Monday, 16 March 2026 (extended from Friday, 23 January 2026)

Category: Technical

Requester: ICANN organization

ICANN organization contact(s):
francisco.arias@icann.org

Open Proceeding Link:
https://www.icann.org/en/public-comment/proceeding/name-collision-ipv6-research-study-20-10-2025

Outcome:

Based on the feedback received during the Public Comment proceeding and as a result of internal review, ICANN org has decided to not perform controlled interruption with IPv6 in the 2026 Round. Additional work is planned and ICANN will consider the topic again once the Internet Engineering Task Force (IETF) has developed a standardized solution.

Section 1: What We Received Input On

ICANN org sought input on the Controlled Interruption IPv6 Research Study Summary Report, which proposed the use of ffff::127.0.53.53 in the AAAA record for future controlled interruption activities.

Section 2: Submissions

Organizations and Groups:

Name	Submitted by	Initials
Registries Stakeholder Group (RySG)	publiccomments@rysg.info	RySG
Policy staff in support of the At-Large Advisory Committee (ALAC)	staff@atlarge.icann.org	ALAC
Root Server System Advisory Committee	rssac-staff@icann.org	RSSAC

Individuals:

Name	Affiliation (if provided)	Initials
MD Imran Hossen	N/A	MDIH
Eric Vyncke	Cisco	EV
Nick Hilliard	N/A	NH
Ted Lemon	N/A	TL
Jen Linkova	N/A	JL
Jordi Palet Martinez	N/A	JPM
Brian Carpenter	Retired	BC
Mark Smith	IETF	MS
Michael Richardson	N/A	MR

Section 3: Summary of Submissions

Input Received	ICANN org input
The **Registries Stakeholder Group (RySG)** agrees that the need for an IPv6 Controlled Interruption methodology has increased substantially since the 2012 Round of New gTLDs. The RySG requests that ICANN investigate the impact on the NCAP Report and propose an implementation plan to be reviewed by the community. Pending the review of the implementation plan, the RySG agrees that, based on the results of the research studies, **the use of Candidate 1 (ffff::127.0.53.53) (also represented as (::ffff:7f00:3535)) as the AAAA record in the next round of Controlled Interruption activities is a good choice**.	ICANN appreciates the comment. However, based on other input received, ICANN will not perform controlled interruption with IPv6 on the 2026 round. ICANN will consider the topic again once the IETF has standardized a solution for this.
The **Root Server System Advisory Committee (RSSAC)** believes that controlled interruption for new gTLDs is a good practice for both IPv4 and IPv6. Furthermore, the RSSAC **has no objections to the IP address**	Please see the response to the RySG comment above.

Input Received	ICANN org input
::ffff:127.0.53.53 being used for IPv6 controlled interruption.	
MD IMRAN HOSSEN comment **supports the selection of ::ffff:7f00:3535 as the IPv6 Controlled Interruption address** based on the study's findings that it is safe, non-routable, consistent with IPv4 CI behavior, and preserves the educational value of CI. The comment highlights concerns with alternative multicast and link-local options and **encourages future collaboration with the IETF** to define a dedicated IPv6 loopback block.	Please see the response to the RySG comment above.
The **At-Large Advisory Committee (ALAC)** supports the development of an IPv6-based Controlled Interruption mechanism but **cannot endorse the use of ::ffff:127.0.53.53 due to significant technical, operational, and standards-related concerns**. As IPv6 adoption grows, relying on a mapped-loopback address risks inconsistent behavior and reduced error transparency for users, especially in IPv6-only environments. ALAC recommends further testing, exploration of standards-aligned alternatives, and strong user-focused guidance before any IPv6 CI approach is adopted.	ICANN recognizes the need to further investigate the impact of address selection for controlled interruption in IPv6-only environments.
Michael Richardson proposes a **PTR like possible-future-tld.icann.org for the 127.0.53.53** to help users of that "string" to understand what is going on.	ICANN agrees that more information to users would be useful. However, as 127.in-addr.arpa is not delegated, adding a PTR is not possible at this time.
Eric Vyncke writes that using ffff::127.0.0.53 is a bad use of ffff:: prefix and **that the IETF intends to shortly have a IETF draft** (and later a RFC) **about specific IPv6 address(es) for very similar/more generic use** (i.e., not only for TLD). So, suggest to **delay any decision until this IETF draft is submitted**.	ICANN plans to engage within the IETF to standardize a suitable solution for controlled interruption. Please also see the response to the RySG comment above.

Input Received	ICANN org input
Brian Carpenter believes that **ICANN are suggesting an IPv6 special-use address**, and that is something to be debated **not in an ICANN process but in an IETF process**. As is recorded in the relevant IANA registry, this is an assignment requiring IETF Review. In other words, ICANN cannot assign ffff:127.0.53.53; only the IETF could do so. The starting point would be an Internet-Draft aimed at the 6MAN working group.	ICANN will engage with the IETF as described above.
Ted Lemon urged ICANN to formally engage with the IETF to come up with a solution to this problem.	ICANN will engage with the IETF as described above.
Jen Linkova believes the decision of what IPv4 and IPv6 addresses can not be made by ICANN, and this Public Comment seems to be a wrong process for making that decision.	ICANN will engage with the IETF as described above.
Jordi Palet Martinez writes that **parameters belong to IETF as part of IETF protocols, and that's the right place for the discussion**, not any Public Comment. ICANN/IANA can't unilaterally consult on those matters.	ICANN will engage with the IETF as described above.
Nick Hilliard refers to the "IETF-ICANN Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority", and writes that if ICANN wants a specific addresses to be reserved, that **needs to be done via publication of an IETF RFC**, exclusively using IETF processes. At a practical level, the starting point for the suggestion to use ::ffff:127.0.53.53 or ::ffff:7f00:3535 would be to write an Internet Draft to be published as an appropriate RFC to reserve the IPv4 address 127.0.53.53. Once IPv4 registration is complete, the ipv6 registration should be straightforward	ICANN will engage with the IETF as described above.

Input Received	ICANN org input
Mark Smith believes this **proposal needs to be made via an Internet Draft** submitted to the IETF v6ops working group. **Only IANA can assign special purposes to IPv4 and IPv6 addresses** after IETF review and approval.	ICANN will engage with the IETF as described above.

Section 4: Analysis of Submissions

#	Area	Input Received	Language updated? Y/N	If YES, what will the changes be? If NO, why? (rationale)
1	Overview	ICANN org internal review has noted that IPv6 only embedded devices were not tested as part of the research study.	Y	A section was added for transparency so that those who review will know that IPv6 only embedded devices were not tested as part of the research study.

Section 5: Next Steps

1. ICANN org will publish an updated version of *ICANN Controlled Interruption IPv6 Research Study - Summary Report.*
2. ICANN org will perform controlled interruption only with IPv4 in the 2026 Round.
3. ICANN org may consider the use of IPv6 for controlled interruption again once the IETF has developed a standardized solution.

ICANN Controlled Interruption IPv6 Research Study - Summary Report

March 10, 2026

Overview

Controlled Interruption is a phase in the establishment of a new generic top-level domain that is designed to address the risk of Name Collision. During Controlled Interruption, certain DNS resource records are published at and below the gTLD name that are designed to interrupt resolution processes in such a way as to minimize any harm that arises from such interruption.

Controlled Interruption uses A resource records containing the IPv4 address `127.0.53.53`. This address is within the `127.0.0.0/8` prefix, which is used for “loopback” interfaces (see RFC 1122, Section 3.2.1.2). The use of this prefix ensures that any application that uses the result of a DNS query that returns this IPv4 address will not initiate a network connection. `127.0.53.53` is used instead of `127.0.0.1` so that if a user or administrator performs a web search for this address, they are more likely to be shown links to the Name Collision resources on ICANN’s web site.

When the concept of Controlled Interruption was originally developed in 2014, no suitable equivalent address could be found for IPv6-enabled hosts. While this was noted as a limitation, at the time the impact was limited since fewer than 5% of internet hosts supported IPv6. In the intervening decade, IPv6 adoption has accelerated, and now more than 40% of all internet hosts have IPv6 connectivity. As a result, the lack of an IPv6 solution for Controlled Interruption has a much greater impact.

ICANNs preferred approach would be to use an IPv6 loopback address analogous to the existing IPv4 `127.0.53.53` address, however, IPv6 has only a single loopback address allocated (::1 [RFC 4291]). Two proposals within the IPv6 Operations working group at the IETF to assign a larger loopback prefix have not gained consensus and as a result there is still no

direct equivalent IPv6 address available today. Should such an address become available in the future ICANN would intend to utilize it for Controlled Interruption. In lieu of that, and with a recognition of the current impact of not publishing a AAAA record for Controlled Interruption, an alternative option that can be deployed as an interim solution is highly desirable.

A new research study has been performed to identify one or more IPv6 addresses that may be suitable for use during Controlled Interruption. This study involved a review of the IANA registries for IPv6 to produce a list of candidate addresses, followed by technical tests of popular end-user operating systems to determine whether or not DNS lookups that produce responses containing these addresses result in external network traffic.

Note on Limitations of this Study

IPv6-only embedded devices have NOT been tested as part of this research study. Such devices typically have limited IPv6 stacks and may behave differently than non-embedded operating systems. They also tend to have very limited logging or troubleshooting capabilities. As a result, connection failures due to controlled interruption may not be visible to a user or administrator, and therefore are less likely to be reported to ICANN. Further work is needed to evaluate the interaction of controlled interruption and such devices.

Research Study

This document is part of a set of documents covering the results of the study:

- Research Study Stage 1 Report
- Research Study Stage 2 Report
- Research Study Summary Report (this document)

An overview of the results of Stage 1 and 2 are given below.

Stage 1

The study involved a review of all the RFCs published by the IETF that establish or discuss registrations in the Internet Protocol Version 6 Address Space and IANA IPv6 Special-Purpose Address Registry registries, to develop a list of candidate address prefixes. A prefix was considered a candidate if the specifications indicate that packets with a destination address within that prefix would remain local to the host (i.e., packets will not be transmitted outbound from the host).

A range of first class candidate prefixes were identified including

- IPv4 mapped IPv6 address (::ffff:0:0/96) [RFC4291]
- Dummy IPv6 addresses (100:0:0:1::/64) [RFC9780]
- Documentation prefixes (2001:db8::/32 and 3fff::/20) [RFC3849] and [RFC9637]
- Various pre-defined multicast addresses e.g. ff01::1, ff02::1 [RFC4291]

Additionally some second class prefixes were also identified (which didn't meet the specific requirement above, but were included in the testing for completeness)

- Partially unallocated address space (::/128) [RFC4291]
- Unique-Local Unicast (fc00::/10) [RFC4193] [RFC8190]
- Link-Local Unicast (fe80::/10) [RFC4291]

This set of candidate prefixes was put through basic testing to observe the traffic generated and only 3 candidate prefixes generated no network traffic in these tests:

- IPv4 mapped IPv6 address (::ffff:0:0/96) [RFC4291]
- Various pre-defined multicast addresses e.g. ff01::1, ff02::1 [RFC4291]
- Link-Local Unicast (fe80::/10) [RFC4291]

Stage 2

This subset of candidate prefixes were then put through more extensive testing in a range of benchtop tests across a matrix of factors (including but not limited to):

- Popular end-user operating systems (all not end-of-life versions)
  - Desktop/server OS's (e.g. Ubuntu, macOS, Windows, RedHat, *BSD)
  - Mobile platforms (e.g. iOS, Android)
- Various applications:
  - Command line tools (e.g. `ssh`, `curl`, `nc`, `openssl s_client`)
  - Popular browsers (e.g. Chrome, Safari, Firefox)
  - Proxies and mail servers (e.g. `postfix`, `sendmail`, `nginx`, `HAProxy`)
- Dual stack and IPv6 only environments
  - Note that in the IPv6 only environments tested the hosts still had an IPv4 loopback interface.

The testing involved the following steps:

1. Invocation of the application with a test name (which resolved to the candidate prefix).
2. Traffic capture of the resulting network and loopback traffic
3. Analysis of the traffic to determine if DNS resolution was attempted and also to identify any traffic generated by the application on either interface.
4. Analysis of the application behaviour i.e. connection attempt, timeouts or error messages.

Results

The study concluded that 2 types of candidate prefix met the requirements:

Candidate Type	Candidate Prefix	Description
Mapped Loopback	`::ffff:7f/104`	"IPv4-mapped IPv6 addresses" [Section 2.5.5.2 of RFC4291] corresponding to the IPv4 loopback address space 127.0.0.0/8

Candidate Type	Candidate Prefix	Description
Pre-defined Multicast	`ff01::1, ff01::2, ff02::1,...`	Several of the pre-defined multicast addresses with limited scope [Section 2.7.1 of RFC4291]

It was observed in the Stage 2 testing that while the Link Local Unicast candidate prefix generated no traffic with a destination IP address of the candidate address, in certain scenarios ICMPv6 Neighbour Solicitation traffic was generated and so this candidate prefix was ruled out.

From the two remaining types, two specific candidate prefixes were tested across the matrix of factors and are determined to be suitable for use in Controlled interruption AAAA records based on meeting the technical criteria (i.e., packets will not be transmitted outbound from the host).

Candidate	Candidate Prefix	Description
1	`::ffff:7f00:3535`	"IPv4-mapped IPv6 address" [Section 2.5.5.2 of RFC4291] corresponding to the IPv4 address 127.0.53.53
2	`ff01::1`	Node-Local Scope Multicast Address, All Nodes Address [Section 2.7.1 of RFC4291] [IANA]

Of these two, Candidate 1 is preferred as discussed below.

Candidate 1

The address `::ffff:7f00:3535` (also represented as `::ffff:127.0.53.53`) is selected from the Mapped Loopback prefix type since it is the companion address to the existing IPv4 Controlled interruption address `127.0.53.53`.

In testing it behaves similarly (though not identically) to the existing IPv4 Controlled interruption address, in that:

- It generates no packets that are transmitted outbound from the host on the network interface.
- In some test scenarios it generates IPv4 traffic on the loopback interface. This tends to generate connection refused, timeouts or similar errors.
- In other test scenarios it produces an error with no connection attempt such as DNS resolution failure or invalid argument.

As with the existing IPv4 Controlled interruption address, it is anticipated that if a user or administrator performs a web search for this address, they are likely to be shown links to the Name Collision resources on ICANN's web site.

Candidate 2

The Node-Local Scope Multicast Address, All Nodes Address is selected from several pre-defined multicast addresses since it has the narrowest scope of the pre-defined addresses.

In testing it:

- Generates no packets that are transmitted outbound from the host on the network interface.
- Generates no packets on the loopback interface.
- Generates a variety of error messages (connection failures, resolution failures, network unreachable, address not supported, invalid argument).

The major drawback of this address is that it is unlikely to lead a user or administrator performing a web search to the Name Collision resources on ICANN's web site.

Proposal

ICANN proposes to use Candidate 1 (`::ffff:7f00:3535`) as the AAAA record in the next round of Controlled Interruption activities and requests feedback from the community on this.